Анна Алексеевна НОВОСЕЛЬЦЕВА
студентка специальности «Экономическая безопасность»
Тюменского государственного университета, г. Тюмень, anna13102000@gmail.com
Сергей Сергеевич ТУРБЫЛЕВ
студент специальности «Экономическая безопасность»
Тюменского государственного университета, г. Тюмень, turbo1401@icloud.com
Юлия Николаевна РУФ
кандидат экономических наук, доцент, доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, ruf2077@yandex.ru

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК ЭЛЕМЕНТ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В КОММЕРЧЕСКИХ ОРГАНИЗАЦИЯХ

Аннотация. Недобросовестное отношение к защите персональных данных приводит к их утечке и несанкционированному доступу с целью уничтожения, распространения, а также других неправомерных действий с персональными данными. В статье идет речь о персональных данных в коммерческих организациях, рассмотрены возможные риски и угрозы для экономической безопасности организаций, а также законодательство в сфере персональных данных и комплекс необходимых мероприятий для их защиты. Представлена статистика, в том числе по судебным делам, и исследования утечек персональных данных. Определены меры по обеспечению безопасности персональных данных.
Ключевые слова: Персональные данные, конфиденциальная информация, организация, риски, угрозы, утечка информации, экономическая безопасность.

Anna Alekseevna NOVOSELTSEVA
Student of the specialty "Economic Security" at the Tyumen State University, Tyumen, anna13102000@gmail.com
Sergey Sergeevich TURBYLEV
Student of the specialty "Economic Security" at the Tyumen State University, Tyumen, turbo1401@icloud.com
Yulia Nikolaevna RUF
Candidate of Economic Sciences, Associate Professor of the Department of Economic Security, System Analysis and Control, Tyumen State University, Tyumen, ruf2077@yandex.ru

SECURITY OF PERSONAL DATA AS AN ELEMENT OF THE SYSTEM OF ECONOMIC SECURITY IN COMMERCIAL ORGANIZATIONS

Abstract. An unscrupulous attitude to the protection of personal data leads to their leakage and unauthorized access for the purpose of destruction, distribution, as well as other illegal actions with personal data. This article deals with personal data in commercial organizations, considers possible risks and threats to the economic security of organizations, as well as legislation in the field of personal data and a set of necessary measures to protect them. Statistics are presented, including on court cases, and studies of personal data leaks.
Keywords: Personal data, confidential information, organization, risks, threats, information leakage, economic security.

На современном этапе информация является одним из главных аспектов в функционировании каждой организации. Утечка персональных данных наносит финансовый ущерб организации, влечет за собой гражданскую, админи-

стративную, дисциплинарную и уголовную ответственность для тех лиц, которые поспособствовали разглашению персональных данных. А также разглашение персональных данных в некоторых случаях может привести к полной ликвидации организации. Отсюда следует, что исследование эффективных методов защиты персональных данных является актуальным вопросом экономической и информационной безопасности.

Сегодня защита персональных данных является, во-первых, требованием законодательства, которая регулируется: Федеральным законом № 152-ФЗ «О персональных данных», Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом № 249-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», Трудовой кодекс Российской Федерации (гл. 14), а также Гражданский кодекс Российской Федерации. Во-вторых, требованием организации, так, в каждой организации есть информационная система персональных данных, которая требует особого контроля. Например, в организациях назначается лицо, ответственное за организацию обработки персональных данных, которое осуществляет внутренний контроль за соблюдением законодательства, а в крупных компаниях, вдобавок, прибегают к использованию ключ-карт для доступа к данным.

Согласно ст. 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» определение персональных данных включает в себя любую информацию, которая прямо или косвенно позволяет идентифицировать физическое лицо [1]. Персональными данными являются: фамилия, имя, отчество физического лица в сочетании с адресом местожительства или регистрации, дата рождения, социальное, имущественное, семейное положение, сведения о доходах, образовании, профессии, данные паспорта. Также это могут быть биометрические данные: отпечатки пальцев, ДНК и т. п. Специальными могут быть — персональные данные, которые присутствуют в личных делах и медицинских книжках и т. д. Например политические убеждения, хронические заболевания, расовая и национальная принадлежности, вероисповедание и др.

В соответствии со спецификой своей деятельности, организации могут использовать данные различных категорий субъектов: коммерческие организации могут обрабатывать персональные данные как работников, так и клиентов, например, службы доставки и т. д. Говоря о категориях, можно отметить определенную категорию лиц, которые не относятся ни категории клиентов, ни категории работников компании. К ним относятся соискатели, которые претендуют на место в организации.

Требования законодательства, а также внутренняя политика организации регулируют комплекс мероприятий по защите персональных данных. В соответствии с требованиями законодательства (ст. 19 «Закон о персональных данных») оператор персональных данных обязан выполнить ряд как организационных, так и технических мер, касающихся процессов обработки персональных данных (рис. 1).

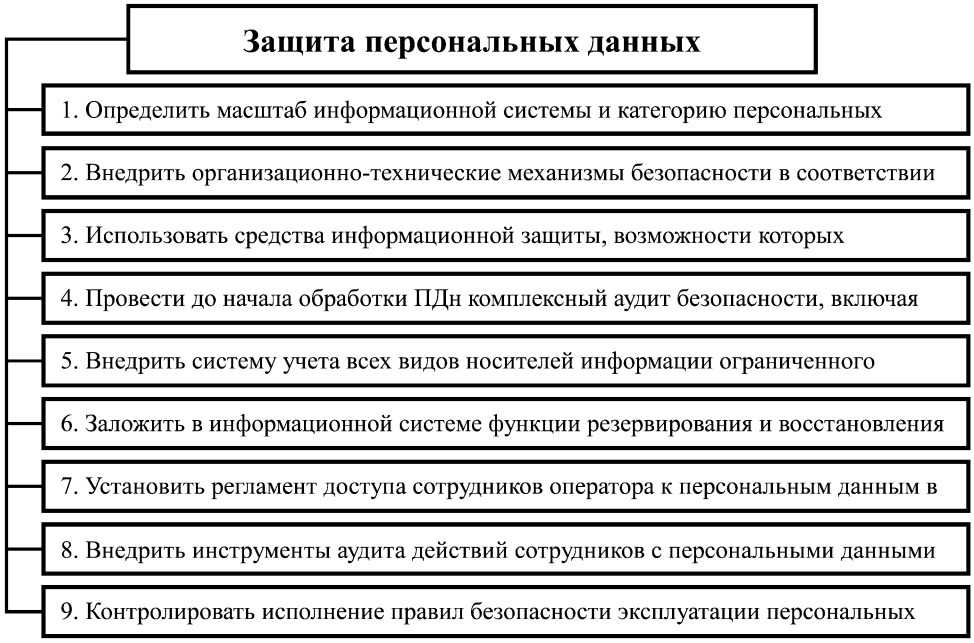

Рис. 1. Комплекс мероприятий по защите персональных данных

Источник: [2].

Оператором персональных данных может выступать как государственный или муниципальный орган, так и физическое или юридическое лицо, которые организуют и осуществляют обработку персональных данных, определяют цели обработки персональных данных и их содержание.

Сбор персональных данных можно осуществлять только с разрешения пользователя (в коммерческих организациях это сотрудники и клиенты) в форме письменного согласия, которая в интернете может быть заменена на электронную форму. Конечно, есть исключения, согласно законодательству, разрешение не требуется, если информация необходима для исполнения полномочий государственных органов, обезличенной статистики, средствами массовой информации и т. п.

Каждой организации необходимо понимать, когда требуется согласие на обработку персональных данных. Для различных категорий субъектов (клиентов, соискателей, работников) определена цель обработки данных. В частности, целью является требование законодательства, в таком случае компания спокойно может собирать персональные данные и обрабатывать их. В случае же, когда цель определена организацией самостоятельно, согласно специфике ее деятельности, необходимо взять согласие на обработку персональных данных [3].

Вне зависимости от ситуации, субъект вправе сделать запрос у оператора, где и какие именно данные на него хранятся, а также если информация некорректна или устарела, то он может потребовать удалить ее.

В отношении персональных данных существует опасность некоторых условий или же воздействующих факторов, которая заключается в несанкционированном доступе третьих лиц к защищаемым персональным данным, изме-

нении, уничтожении, распространении, а также других неправомерных действий с персональными данными [4]. Такие условия и воздействующие факторы являются угрозами для экономической безопасности коммерческих организаций.

К типичным угрозам можно отнести:

– утечки данных по техническим каналам;

– несанкционированный доступ (действия как внутренних, так и внешних нарушителей);

– специальные воздействия, например, интеграция сетевого вредоносного софта, выявление паролей или перехват трафика.

В результате угроз возникают многочисленнее риски для организации. Финансовые потери от утечки могут быть прямыми и косвенными. Одним из косвенных может стать репутационный риск, при котором происходит отток клиентов и снижение притока новых, что явно повлияет на прибыль компании. К прямым же относятся потеря кадров, потеря ноу-хау, штрафы и выплаты компенсаций пострадавшим вследствие утечки персональных данных. Такие суммы могут существенно повлиять на финансовое состояние компании. Такая практика широко распространена в зарубежных странах, в России законодательством предусмотрены небольшие штрафы и компенсации. Стоит отметить, что небольшими такие штрафы могут являться для крупных корпораций, в случае, если небольшая организация столкнется с множественными исками в суд — это может привести к достаточно большим потерям или же к банкротству. Вдобавок придется усовершенствовать защиту информации, что тоже недешево. По этой причине компаниям следует ответственнее относиться к защите данных пользователей и компании. Для обеспечения безопасности персональных данных требуются специалисты, разбирающиеся в требованиях законодательства, организационных и технических составляющих.

Коммерческие организации, являясь также операторами персональных данных, нередко сталкиваются с утечками информации. Такое происходит как по вине сотрудников, так и в результате кибератак на организацию.

В основном защита от утечки персональных данных клиентов или работников организации является второстепенной задачей. Причиной тому отсутствие строгого финансового наказания.

Согласно исследованию уровня информационной безопасности, в компаниях России и СНГ за 2020 год, с утечками информации столкнулись 58% опрошенных компаний, из них 21% столкнулись с потерей персональных данных [5].

Утечка персональных данных составляет 33% от всех сливов (рис. 2).

Рис. 2. Утечка персональных данных в частных компаниях за 2020 г.

Источник: составлено автором по данным [5, с. 13].

Такие утечки фиксируют примерно четверть организаций. Число остается относительно постоянным каждый год. Причиной тому то, что обеспеченность компаний специализированным программным обеспечением, которое могло бы позволить предотвратить и выявить сливы и утечки, растет довольно медленно. Это позволяет удерживать число инцидентов, но не меняет ситуацию целиком и полностью.

Рассмотрим судебную статистику. По официальным данным Судебного департамента общее количество дел по ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных», 13.12 «Нарушение правил защиты информации», 13.13 «Незаконная деятельность в области защиты информации» и 13.14 «Разглашение информации с ограниченным доступом» по итогам 2021 г. составило 386 дел, из которых 31 дело перешли с 2020 г., и 355 из 391 дела поступили в 2021 г. [6].

Число рассмотренных дел в судах в 2021 г. по сравнению с 2020 г. снизилось на 26% (рис. 3). В первом полугодии 2020 г. было рассмотрено 524 дела, 496 из которых новые и 28 перешли с 2019 г. [6].

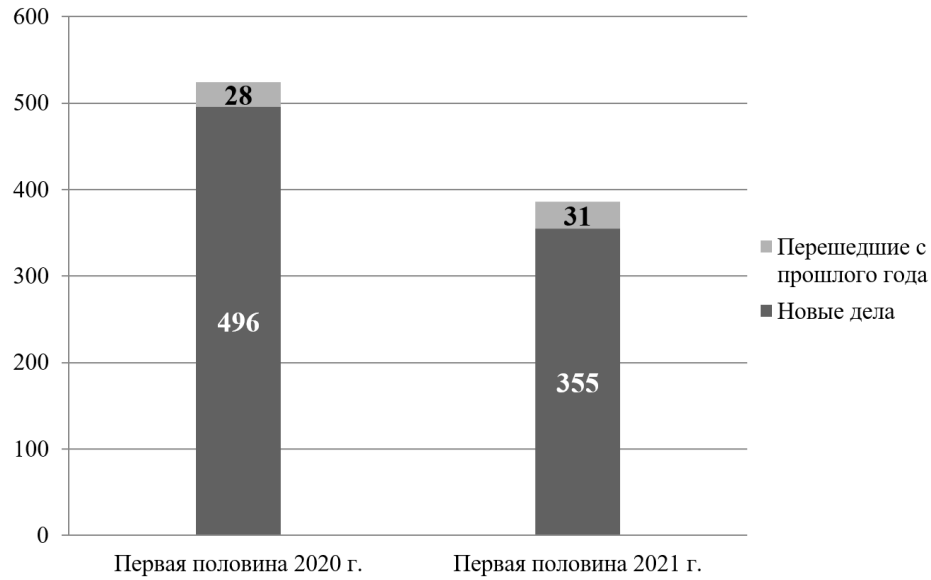

Рис. 3. Число рассмотренных дел в судах за первую половину 2020 г. и первую половину 2021 г.

Источник: составлено автором по данным [6, с. 7].

Большинство нарушителей имели легитимный доступ к конфиденциальной информации, которая впоследствии была раскрыта, то есть были сотрудниками организаций. Это говорит о том, что по сей день часть утечек информации происходят по вине внутренних пользователей. Именно поэтому на сегодняшний день по-прежнему существует необходимость в усилении средств защиты в данном направлении.

Также положительной тенденцией в период с 2019 по 2021 г. для компаний является снижение инцидентов по размещению паспортов безопасности социальных объектов. Но в то же время возросло количество случаев, связанных с размещением персональных данных в сети и их незаконной передачей через мессенджеры.

В настоящее время утечки информации все больше привлекают внимание средств массовой информации. Имиджевый риск, а именно вероятность попасть в публикации средств массовой информации при случившемся инциденте, является одним из главных рисков, мотивирующих компании заниматься сохранностью персональных данных.

Одним из наиболее ярких примеров имиджевого риска является история с утечкой персональных данных коммерческой организации ООО «Яндекс.Еда» [7].

Вследствие массовых кибератак на веб-ресурсы Российской Федерации множество личных данных пользователей было незаконно выложено в сеть. Компания «Яндекс» сообщила об утечке данных пользователей «Яндекс.Еды» 1 марта 2022 года. По заявлению компании, утечка произошла по вине одного из сотрудников организации. Также было отмечено, что утечка не коснулась банковских, платежных и регистрационных данных пользователей, т.е. логинов и паролей. Известно, что инсайдер предоставил открытый доступ архива, содержащего 50 миллионов строк: имена клиентов, телефонные номера из РФ, Беларуси и Казахстана, а также адреса, состав, комментарии и даты заказов. Спустя время злоумышленники, воспользовавшись ситуацией, запустили сайт с визуализацией, где привязали данные пользователей «Яндекс.Еды» к интерактивной карте.

В связи с произошедшим инцидентом «Яндекс.Еда» отменили ручную обработку, к тому же добавили, что за прошедшие недели с начала инцидента команда свела к минимуму количество сотрудников, имеющих доступ к конфиденциальным данным. Данные были перемещены в более защищенное хранилище. Также организация сообщила, что в дальнейшем клиенты смогут отслеживать и удалять накопленные данные в сервисе [8].

Данная ситуация значительно повлияла на имидж компании, в связи с этим происшествием многие клиенты стали отказываться от предоставляемых услуг сервиса, некоторые клиенты компании и подали коллективный иск против «Яндекс.Еды» о взыскании компенсации морального вреда, требующий возместить по 100 000 руб. за утечку их персональных данных [9]. Также компании грозит штраф по ч. 1 ст. 13.11 КоАП в размере от 60 до 100 тыс. руб., точную сумму штрафа определит суд [10].

С учетом вышеизложенного, требования по обработке персональных данных можно разделить на три блока [1]: правовые, организационные и технические меры защиты.

В качестве рекомендаций для обеспечения экономической безопасности организации можно выделить следующее:

Во-первых, компании необходимо обеспечить правовые меры защиты персональных данных, то есть определить, как будут выполняться требования законодательства и, соответственно, отразить это во внутренних нормативных актах.

Во-вторых, принять должные организационные меры, например, опубликовать Политику в отношении обработки персональных данных.

В-третьих, обеспечить технические меры защиты.

Остановимся подробнее на технических мерах защиты. Они связаны с использованием высокотехнологичных средств защиты информации. К ним можно отнести:

– антивирусы, например, Kaspersky Internet Security, Avast Premium Security и др.;

– средства криптографической защиты информации, например, КриптоПро CSP, VipNet CSP и др.;

– системы предотвращения утечек информации, например, InfoWatch Prediction, InfoWatch Person Monitor, SearchInform DPL в облаке и др.

Сегодня для исключения случаев утечки информации в коммерческих организациях также устанавливают специальное программное обеспечение.

Рекомендуемые приложения для защиты данных: StaffCop, IBM QRadar SIEM, Rapid7 InsightlDR.

Данные приложения являются одними из лучших решений безопасности, которые способны обеспечить защиту данных компании, выявить угрозы и вирусные атаки, а также отреагировать на несанкционированный доступ.

Учитывая вышеприведенные данные, можно сделать вывод, что защита персональных данных в коммерческих компаниях является одним из важнейших элементов экономической безопасности организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (последняя редакция) // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 12.03.2022).
2. Защита персональных данных // ООО «СёрчИнформ»: [сайт]. 2022. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/ (дата обращения: 10.04.2022).
3. Пять базовых принципов закона о персональных данных // СКБ Контур: [сайт]. [дата публ. 24.01.2022]. 1988–2022. URL: https://kontur.ru/articles/1293 (дата обращения: 12.03.2022).
4. Угрозы безопасности персональных данных // Центр безопасности данных: [сайт] 2011-2022. URL: https://data-sec.ru/personal-data/threats/ (дата обращения: 10.04.2022).
5. Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 г. // ООО «СёрчИнформ». 2021. 42 с.
6. Исследование судебной практики по административным правонарушениям, связанным с безопасностью персональных данных и защитой информации в 2021 г. // Экспертно-аналитический центр InfoWatch. 2022 г. 24 с.
7. «Яндекс.Еда» выявила утечку личных данных пользователей, которые не касались платежей // ТАСС, информационное агентство: [сайт]. [дата публ. 01.03.2022]. URL: https://tass.ru/ekonomika/13921381 (дата обращения: 26.03.2022).

8. Пользователи «Яндекс.Еды» смогут управлять хранением персональных данных // ТАСС, информационное агентство: [сайт]. [дата публ. 24.03.2022]. URL: https://tass.ru/ekonomika/139213811293 (дата обращения: 26.03.2022).
9. Недостойная компенсация: чем интересен коллективный иск к «Яндекс.Еде» // АО «АС Рус Медиа». Forbes.ru: [сайт]. [дата публ. 01.04.2022]. 2021-2022. URL: https://www.forbes.ru/mneniya/460977-nedostojnaa-kompensacia-cem-interesen-kollektivnyj-isk-k-andeks-ede (дата обращения: 03.04.2022).
10. РКН составил на «Яндекс.Еду» протокол за утечку данных клиентов // ТАСС, информационное агентство: [сайт]. [дата публ. 23.03.2022]. 1991-2022 URL: https://www.interfax.ru/business/830865 (дата обращения: 26.03.2022).